

**REMARKS**

The Applicant and the undersigned thank Examiner Kiss for his careful review of this application. In view of the Request for Continued Examination filed concurrently herewith, Applicant respectfully requests reconsideration of this application in view of the above amendments to claims and the following remarks.

The Examiner has rejected Claims 1-25 based on the Official Action mailed on October 28, 2003. Upon entry of this amendment, Claims 1-25 remain pending in this application and new Claims 29-34 have been added. Applicant has amended Claims 6-9, 13-17, 18, 20, 22 and 25. Claims 1, 11, 18, 20, 22, 26 and 29 are the independent claims of this amended application. It is respectfully submitted that this reply is fully responsive to the issues raised by the Examiner in the October 28, 2003 Official Action.

**Claim Rejections Under 35 U.S.C. § 112**

The Examiner has rejected Claims 6-9 and 13-17 under 35 U.S.C. § 112, second paragraph, based on the assertion that these claims fail to particularly point out and distinctly claim the subject matter of the claimed invention. Applicant has amended Claims 6-9 and 13-17 to address the concerns raised by the Examiner in numbered paragraph 6 of the Official Action.

**Claim Rejections Under 35 U.S.C. § 103**

The Examiner rejected Claims 1, 5, 11-12, and 18-25 under 35 U.S.C. § 103(a) in view of the asserted combination of a 1997 article entitled "Understanding Heuristics: Symantec's Bloodhound Technology" (hereinafter "*UHBST*") with a February 2000 article entitled "Enterprise Anti-Virus Software," by Robert Richardson (hereinafter "*Richardson*"). The Applicant respectfully offer remarks to traverse these pending rejections in view of distinctions between the *UHBST* and *Richardson* references and the inventions as defined by independent Claims 1, 11, 18, 20 and 22.

**Independent Claims 1, 11, 18, 20 and 22 are Distinguishable from the *UHBST* and *Richardson* Articles Because Neither Reference Teaches a Virtual Machine having a Virtual PC and a Virtual Operating System Simulating a Multi-Threaded Operating System**

The present rejection of independent Claims 1, 11, 18, 20 and 22 is respectfully traversed. Neither the *UHBST* reference nor the *Richardson* reference, either singularly or in combination, describes, teaches, or suggests the recitations enumerated by Claims 1, 11, 18, 20 and 22 or the claims dependent therefrom.

As acknowledged by the Examiner, the *UHBST* reference fails to describe the task of initializing a *virtual machine* comprising a *virtual PC* implemented by software simulating functionality of a central processing unit and memory and a *virtual operating system* simulating functionality of a multi-threaded operating system. Moreover, the *Richardson* reference fails to disclose, teach or suggest the operation of a *virtual operating system* simulating functionality of a multi-threaded operating system in connection with a *virtual PC* implemented by software simulating functionality of a central processing unit and memory to form a *virtual machine*.

Applicant respectfully submits that page 2, paragraph 8 of *Richardson* merely discloses the use of a conventional “Windows” emulator in the context of a dynamic heuristic approach to virus scanning. For example, in the absence of a disclosure of the design or structure of this virus scanner, the Windows emulator in *Richardson* could be implemented by a stand-alone software tool used by a laboratory technician to simulate the operation of an infected software program. While the Examiner has pointed to *Richardson*’s brief disclosure of the use of a “Windows” emulator in connection with virus scanning, *Richardson* is silent on the key critical technical issue of how this “Windows” emulator can be used in connection with a virtual PC within the framework of a virtual machine, as required by Claims 1, 11, 18, 20 and 22. The limited technical disclosure of the *Richardson* reference fails to provide an enabling disclosure of the design, structure or operation of a virus scanner using dynamic heuristics.

Neither the *UHBST* article nor the *Richardson* article discloses how to use a virtual operating system simulating a multi-threaded operating system within the operating environment of a virtual machine comprising a virtual PC and a virtual operating system. Indeed, the two references cited by the Examiner describe a pair of completely different operating system environments, as the *UHBST* reference discloses a DOS-based operating system environment, rather than a multi-threaded computing environment, while the *Richardson* reference discloses

the more complex structure of a “Windows” operating system. In the absence of an enabling teaching by either reference on whether or how to implement the modification alleged by the Examiner, the Applicant respectfully submits that one of ordinary skill in the art would not have recognized at the time of the invention to redesign the DOS-based CPU emulator of the *UHBST* reference to operate with the “Windows” emulator of the *Richardson* reference to form the virtual machine of Claims 1, 11, 18, 20 and 22.

In summary Applicant respectfully requests that the Examiner withdraw the rejection of Claims 1, 11, 18, 20 and 22, as well as all claims dependent therefrom.

**The Alleged Combination of the UHBST and Richardson References Fails to Achieve the Inventions of Independent Claims 1, 11, 18, 20 and 22**

Even assuming, for the sake of argument, that the Examiner is correct in his assertion that one of ordinary skill would have recognized a need to modify the *UHBST* CPU emulator with the “Windows” emulator of *Richardson*, neither reference provides an enabling disclosure on how to achieve this modification in a manner that would form an operating version of the inventions of Claims 1, 11, 18, 20 and 22. Contrary to the Examiner’s assertion, the mere addition of a “Windows” emulator to the DOS-based CPU emulator of the *UHBST* reference does not achieve an operating version of invention recited by Claims 1, 11, 18, 20, and 22 because the DOS-based CPU emulator of the *UHBST* reference would be incompatible with the “Windows” emulator of the *Richardson* reference. This alleged modification would result in an inoperative computing system having DOS-based CPU emulator with an incompatible “Windows” emulator rather than the invention defined by the independent claims of the present application. In view of the foregoing, Applicant respectfully requests that the Examiner withdraw the rejection of Claims 1, 11, 18, 20 and 22, as well as all claims dependent therefrom.

**The UHBST and Richardson References Fail to Disclose or Suggest the Use of a Virtual Machine to Analyze Behavior of a Target Program, as recited by Independent Claims 1, 18 and 20 and Dependent Claim 23**

Neither the *UHBST* reference nor the *Richardson* reference discloses or suggests the use of a virtual machine to complete the analysis derived from the results of a virtual execution of that software program. In contrast to the teachings of these references, the inventions defined by

independent Claims 1, 18 and 20 and dependent Claim 23 require virtually executing the target program within a virtual PC and analyzing the behavior of the target program (upon completion of said virtual execution) by using the virtual machine to complete an evaluation of a behavior pattern resulting from virtual execution of that program.

While both references cited by the Examiner acknowledge the application of dynamic heuristics to virus scanning, these references fall short of disclosing the use of a virtual machine to first complete virtual execution of a target program and to thereafter complete an analysis of the results of that virtual execution. The *UHBST* reference discloses the use of a DOS-based CPU emulator to complete the simulated execution of a software program, while the *Richardson* reference describes the application of a “Windows” emulator to execute the software program. Both references are silent to the use of a virtual machine, comprising both a virtual PC and a virtual operating system, to complete an analysis of the results of virtual execution of a software program, as defined by independent Claims 1, 18 and 20 and dependent Claim 23. Indeed, the *UHBST* and *Richardson* references, when viewed in a light most favorable to the position taken by the Examiner, disclose certain components of a virtual machine for executing a target program rather than a virtual machine that completes virtual execution and analysis operations, as required by Claims 1, 18 and 20 and dependent Claim 23.

In view of the foregoing, Applicant respectfully requests that the Examiner withdraw the rejection of independent Claims 1, 18 and 20, as well as all claims dependent therefrom and dependent Claim 23.

**The Examiner has failed to Present a *Prima Facie* Case for Obviousness under Section 103 for Claims 1-10 and Claims 19, 21 and 25 by Asserting that a Claim Recitation is “Inherent” without Presenting a Citation to a Prior Art Reference in support of that Position**

The Examiner has asserted that removing the target program from a virtual PC upon completion of an evaluation of the results of virtual execution of that target program is *inherent* for the invention of independent Claim 1 and has taken *official notice* that it is well known to implement similar recitations for the inventions of dependent Claims 19, 21 and 25. Applicant respectfully traverses this rejection and submits that the Examiner has failed to present a *prima facie* case of obviousness under 35 U.S.C. § 103(a) for these claims in the absence of properly

citing a prior art reference in support of the Examiner's inherency position. See *In re Lee*, 277 F.3d 1343, 61 USPQ2d 1430 (Fed. Cir. 2002) (“[A] determination of patentability must be based on evidence.”).

The Federal Circuit in *In re Lee* held that an Examiner's conclusion of obviousness from “common knowledge and common sense” for one of ordinary skill in the art without any specific hint or suggestion in a particular reference for support of that position is legal error and represents an arbitrary agency action.

When the [Examiner and the Board] rely on what they assert to be general knowledge to negate patentability, that knowledge must be articulated and placed on the record. The failure to do so is not consistent with either effective administrative procedure or effective judicial review. The [Patent Office] cannot rely on conclusory statements when dealing with particular combinations of prior art and specific claims, but must set forth the rationale on which it relies.

*In re Lee*, 61 USPQ2d at 1435.

Applicant respectfully traverses the Examiner's conclusion of inherency and/or Official Notice with respect to his position that “it has been known and practices (sic) to remove undesirable programs from a system to prevent execution, accidental or intentional, of those undesirable programs” within the framework of the invention defined by independent Claim 1 (and all claims dependent therefrom) and dependent Claims 19, 21 and 25. In the absence of the Examiner's citation of a prior art reference in support of the Examiner's conclusion, Applicant respectfully requests that the Examiner withdraw the rejection of these claims.

**Dependent Claims 2-10, 12-17, 19, 21 and 23-25**

Applicant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. Applicant further submits that the recitations of these dependent claims are of patentable significance and reserves the right to present supplemental remarks in support of that position, if necessitated by continued prosecution of this application. In view of the foregoing, the Applicant respectfully requests that the Examiner withdraw the pending rejections of dependent 2-10, 12-17, 19, 21 and 23-25.

**New Claims 26-34**

Applicant respectfully submits that new Claims 26-34 are distinguishable from the prior art cited by the Examiner. Independent Claims 26 and 29 present alternative views of the inventive aspects disclosed by the present application and are patentable over the prior art of record.

**New Independent Claim 26**

New Claim 26 includes the steps of:

- 1) collecting information about the behavior of a target program in response to virtual execution of the target program by a virtual machine;
- 2) collecting information about interrupt call operations that call any interrupt service routine modified by the virtual execution of the target program in response to completing virtual execution of the target program;
- 3) creating a record comprising the information collected about the virtual execution of the target program and the interrupt call operations that call any interrupt service routine modified by the virtual execution of the target program; and
- 4) analyzing the record to identify an occurrence of malicious code behavior by comparing the record to a behavior pattern representative of the operations performed by the malicious code.

**New Independent Claim 29**

Independent Claim 29 includes the steps of initializing a virtual machine for the computer system, where the initializing step comprises the steps of (1) extracting the file structure of a target program and (2) loading the target program into software-simulated memory of a *virtual PC*.

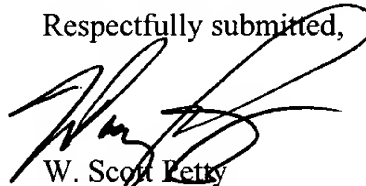
In conclusion, Applicant respectfully submits that the art of records fails to disclose, suggest or teach each and every recitation of new independent Claims 26 and 29 and all claims dependent therefrom. Applicant requests that the Examiner pass these claims to allowance in view of the clear distinctions between the inventions defined by the recitations of Claims 25-34 and the prior art of record.

**CONCLUSION**

The foregoing is submitted as a full and complete response to the Office Action mailed on October 28, 2003. The Applicant and the undersigned thank Examiner Kiss for his consideration of these remarks. The Applicant has amended certain claims and has submitted remarks to traverse the rejection of Claims 1-25. Concurrently herewith, Applicant has submitted a Request for Continued Examination and a Request for an Extension of Time. The Applicant respectfully submits that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2888.

Respectfully submitted,



W. Scott Petty  
Reg. No. 35,645

King & Spalding LLP  
191 Peachtree Street, N.E.  
Atlanta, Georgia 30303-1763  
telephone: (404) 572.4600

K&S File No. 05456-105041